☐ YOU WERE CALLED BY— ☐ YOU WERE VISITED BY—

OF (Organization)

☐ PLEASE CALL → PHONE NO. CODE/EXT. _____ ☐ FTS

☐ WILL CALL AGAIN ☐ IS WAITING TO SEE YOU

☐ RETURNED YOUR CALL ☐ WISHES AN APPOINTMENT

MESSAGE

TC Interface B

210-8093-A

STAT

RECEIVED BY	DATE	TIME

PROPOSED CSP BUDGET HEARING

ISSUE: Due to the allocation of resources in the GDIP, should the operational management and control of the Communications Support Processor be transferred from the joint sponsorship of Air Force Intelligence and DIA to management by the Air Force Communications Command?

BACKGROUND: The Communications Support Processor (CSP) was originally developed by Air Force Intelligence to support a Strategic Air Command (SAC) requirement for an automated message handling capability to process electrically disseminated Sensitive Compartmented Intelligence (SCI), non-SCI intelligence, and operational messages from worldwide locations. Since the mid 1970s, CSP has been enhanced and it has been adopted as a DoDIIS standard product. It is currently installed at approximately 25 locations from Europe to the Pacific, including the White House. CSP allows an organization to receive and transmit messages through both the SCI and non-SCI components of the AUTODIN network. CSP is one of the few processing systems that has been certified for this type of operation. It was built for the Air Force and is maintained under contract by INFORMATICS. The system is certified by DCA for non-SCI message processing and by DIA for SCI message processing. A key feature of its security capabilities is tight configuration control, which is centrally mangaged by INFORMATICS in the Washington, D.C. area and controlled by Air Force Intelligence and DIA. This includes the requirement to have one full time INFORMATICS employee in residence at each CSP location. All changes to CSP must be performed by this representative. Field components are authorized to make only those changes which have been developed and thoroughly tested in Washington--and then certified by Air Force Intelligence and DIA. This tight control procedure has been necessary to insure operational and security integrity. CSP's performance in this regard has been outstanding; however, there are indentified shortfalls in the security of CSP which are being corrected with funding identified under the DCI's COMPUSEC project. CSP is a DCI "critical system".

CSP has been so successful that there are approximatley 100 pending requests for installation of the equipment at DoD and non-DoD locations. The Air Force Intelligence and DIA staffs that has maintained control over CSP are no larger than when the CSP effort first began. Although there have been program and budget requests for additional contract and government personnel resources to maintain control over CSP, these requests have largely been denied. Approximately 30 of these new requests are to use CSP in a totally non-SCI message processing environment as an enhancement effort to upgrade DoD message processing capabilities. Under its current configuration control procedures, these CSP systems must be fielded under the same rigid standards that are imposed on SCI processing systems. The reason for this is that the security features of CSP for both SCI and non-SCI processing are not separable in the processor (i.e., both the security and the functional capabilities to allow SCI and non-SCI message processing are embedded). The demand for this capability has been so great that the Commander, Air Force Communications Command has offered to assume the operational control of CSP (vice Air Force Intelligence and DIA). This offer is apparently under consideration.

SECURITY CONCERN: The resource implications of a shift in operational control of CSP from Air Force Intelligence to Air Communications Command are that GDIP funding for CSP would be assumed by program two. If this occurs, there are implications regarding the control over maintenance of those security features within CSP that currently provide protection of SCI materials. The DCI expressed great concern over a compromising security incident in which a message processing system similiar to CSP incorrectly routed highly sensitive SCI messages to non-SCI users on AUTODIN. One major conclusion of the investigations that followed was that adequate security features had not been maintained by the non-intelligence activity that provided configuration management for the system. As a result of this incident, the DCI directed senior intelligence officers to re-assume their responsibilities for the control and protection of sensitive intelligence information. In his role as the SPINTCOM manager, the Director of DIA is responsible for the security of CSP.

POSSIBLE OPTIONS: Based on informal discussions with Air Force Intelligence and DIA representatives, three options are being considered regarding this issue.

Option I - Provide increased GDIP and/or TIARA funding and manpower to Air Force Intelligence and DIA so that current configuration support and management control procedures will be sufficient to satisfy all outstanding requirements.

Option II - Transfer the configuration support and management control of CSP to the Air Force Communications Command and provide for some type of security verification and accreditation procedures by Air Force Intelligence, DIA, and the DCI via Memoranda of Understanding (MOU).

Option III - Transfer a baseline version of CSP to the Air Force Communications Command for configuration support and management control of all installations that have non-SCI message processing requirements. Maintain Air Force Intelligence and DIA configuration support and mangement control of CSP installations that require SCI and/or SCI and non-SCI message processing support.

REQUEST FOR HEARING: Request that a program and budget hearing on this issue be convened as soon as possible and that all the options being considered for this issue by Air Force Intelligence and DIA be presented and summarized for the ICS with appropriate consideration of the following items:

The name and locations of all current CSP installations and those programmed (or offically requested) for installation over the next five years. (Highlighting those that process either/both SCI and non-SCI messages)

The estimated resources required to maintain the current number of installations under the existing Air Force Intelligence and DIA configuration management effort and the resource requirements for fielding all requested systems using the current AFIS and DIA procedures.

The security control procedures to be used by Air Communications Command if CSP management and funding are assumed by AFCC, including Air Intelligence and DIA roles in certification and recommendations for DCI accreditation of the multi-level security processor. Under the DCI's policy for "critical systems", the DCI must accredit multi-level systems.

What new security roles and responsibilities have been deliniated for the following areas:

Reporting incidents/compromises
Investigating incidents
Approving system operational use

Will Air Force Communications Command maintain one or two versions of CSP?

What mechanisms must be in place to insure DoDIIS CSP requirements are met?

Will Air Force Communications Command continue the testing procedures which currently include the participation of DCA and DIA personnel? Who has responsibility and authority to approve for operational use?

What is the status of and what are the future plans for the AFIS High Order Language (HOL) effort for CSP?

What impact does the AFIS HOL effort for CSP have on this issue and what would be the impact on the AFIS HOL effort if CSP were to be transferred to the Air Force Communications Command?

What are the alternatives regarding this issue and what are the estimated resource implications?

What are Air Force Intelligence and DIA concerns and recommendations regarding this issue?

Identify the role CSP plays in SPINTCOM?

What are the Director, DIA responsibilities for management of the DoD SPINTCOM network?